EDELSBERG LAW, P.A.
Scott Edelsberg, Esq. (CA Bar # 330090)
scott@edelsberglaw.com
1925 Century Park East, Suite 1700
Los Angeles, CA 90067
Telephone: (305) 975-3320

Counsel for Plaintiff

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF CALIFORNIA
FRESNO DIVISION

AQUELIA WALKER, *Individually and On Behalf of All Others Similarly Situated*,

Plaintiff,

v.

RADNET, INC.,

Defendant.

Case No.

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

CLASS ACTION COMPLAINT

Plaintiff Aquelia Walker, on behalf of herself and all others similarly situated, files this Complaint against Defendant RadNet, Inc. ("RadNet" or "Defendant"). Plaintiff's allegations are made on personal knowledge as to Plaintiff and Plaintiff's own acts and upon information and belief as to all other matters.

I. NATURE OF THE ACTION

1. This is a medical privacy class action complaint against RadNet, Inc., as the owner of *radnet.com*, for knowingly and repeatedly intercepting, and disclosing to a third party, Meta Platforms, Inc. ("Facebook"), confidential patient communications and data from RadNet's website containing its patients' personally identifiable information ("PII") and/or statutorily-protected patient health information ("PHI") (together, "User Data") without their knowledge, authorization, or consent, in violation of various state laws, the California constitution, and as well as Defendant's privacy policy with its patients.

2. Like many other hospitals and healthcare providers, RadNet encourages patients to use its website and "secure" online patient portal to communicate with RadNet. Plaintiff and Class Members used *radnet.com* to communicate with their doctors, view lab results, schedule medical appointments, and find treatment options.

3. Patients who exchange communications with RadNet have a reasonable expectation of privacy that their personally identifiable data and the content of their

communications will not be intercepted, transmitted, re-directed, or disclosed by RadNet to third parties without the patient's knowledge, consent, or authorization.

4. Defendant aids, employs, agrees, and conspires with Facebook, through the use of the Facebook Pixel, to intercept communications sent and received by Plaintiff and Class Members, including communications containing protected medical information.

5. The Facebook Pixel is a code Defendant installed on its website and patient portal allowing it to collect and transmit patients' communications containing personally identifiable, sensitive medical information. More specifically, it automatically intercepts and transmits protected medical information, including, but not limited to diagnoses, treatment information, lab results, medications, and appointment times. This occurs even when the patient has not shared (nor consented to share) such information.

6. Unbeknownst to Plaintiff and Class Members, and pursuant to the systemic process described herein, whenever a patient uses RadNet's website and patient portal, patients' private and protected communications with RadNet were automatically transmitted and communicated to Facebook, alongside other information—including diagnoses, treatment information, lab results, medications, appointment times, and patients' unique Facebook ID ("FID")—as a result of Defendant's decision to install and use tracking pixels on its website.

7. Importantly, because the patient's FID uniquely identifies an individual's Facebook user account, Facebook—or any other ordinary person—can use it to quickly and easily locate, access, and view patients' corresponding Facebook profile. Put simply, Facebook Pixel grants Facebook knowledge of the private medical information of RadNet's patients communicated on the *Radnet.com* site.

8. Defendant disregarded Plaintiff's and hundreds of thousands of other patients' statutorily protected, constitutional, and common law privacy rights by intercepting and releasing their sensitive personal medical information to Facebook. As a result, Defendant violated state statutes, including the California Invasion of Privacy Act, Cal. Penal Code §§ 630 *et seq.* ("CIPA"), and the California Confidentiality of Medical Information Act, Cal. Civil Code §§ 56 *et seq.* ("CMIA"). Defendant's conduct also constitute an invasion of privacy under California's Constitution and the common law, and a breach of contract.

9. Accordingly, Plaintiff brings this class action for legal and equitable remedies to redress and put a stop to Defendant's practice of intentionally disclosing its patients' User Data to Facebook in knowing violation of state privacy laws, the California constitution, and its privacy policy.

II. JURISDICTION AND VENUE

10. Court has jurisdiction over the subject matter of this action pursuant to 28 U.S.C. § 1332(d)(2), because the matter in controversy exceeds $5,000,000,

exclusive of interest and costs, and is a class action in which at least one member of the class is a citizen of a different State than Defendant. The number of members of the proposed Classes in aggregate exceeds 100 users. 28 U.S.C. § 1332(d)(5)(B).

11. Venue is appropriate in this District pursuant to 28 U.S.C. § 1391 because Defendant resides in and is subject to personal jurisdiction in this District. Venue is also proper because a substantial part of the events or omissions giving rise to the claim occurred in or emanated from this District.

III. DIVISIONAL ASSIGNMENT

12. Assignment to the Fresno Division is appropriate because Plaintiff is domiciled in Fresno County and a substantial part of the events or omissions giving rise to this action occurred in Fresno County.

IV. PARTIES

13. Defendant RadNet, Inc., is a Delaware corporation with its principal place of business in Los Angeles, California. RadNet is a provider of outpatient diagnostic imaging services, with locations across California and in Arizona, Florida, Delaware, Florida, Maryland, New Jersey, and New York. RadNet was founded in 1984 as a small radiology imaging center in Los Angeles. Now, with over 332 imaging centers and thousands of patients, RadNet's estimated annual revenues exceed $1 billion.

14. Plaintiff Aquelia Walker is an adult citizen of California and is domiciled in Clovis, California. Plaintiff has been a patient of RadNet since at least

2013 and continues to remain a patient to this day. At all relevant times, Plaintiff has had a Facebook account.

15. Plaintiff entrusted her User Data to Defendant as a condition of receiving Defendant's healthcare services.

16. To receive healthcare services from Defendant, and at Defendant's direction, Plaintiff accessed Defendant's website. From 2013 to the present, Plaintiff used RadNet's website to manage her appointments, access testing and imaging results, view doctor's notes, message healthcare providers, and review medications and treatment information.

17. Plaintiff reasonably expected that her online communications with Defendant were confidential, solely between herself and Defendant, and that such communications would not be transmitted to or intercepted by a third party.

18. Plaintiff provided her User Data to RadNet and trusted that the information would be safeguarded according to its privacy policy and state and federal law.

19. To access RadNet's patient portal, Plaintiff provided, among other information, her name, date of birth, full address, email address, phone number, IP address (which informs RadNet as to the city and zip code she resides in as well as her physical location), and any cookies associated with her device.

20. Plaintiff never consented, agreed, authorized, or otherwise permitted RadNet to disclose her User Data to Facebook. Plaintiff has never been provided any

written notice that RadNet discloses its patients' User Data, or any means of opting out of such disclosures of her User Data. Nonetheless, RadNet knowingly disclosed Plaintiff's User Data to Facebook.

21. By law, Plaintiff is entitled to privacy in her User Data and confidential electronic communications. RadNet deprived Plaintiff of her privacy rights when it: (i) implemented a system that surreptitiously tracked, recorded, and disclosed Plaintiff's and other and other online patients' confidential communications and User Data; (2) disclosed patients' protected information to Facebook; and (3) undertook this pattern of conduct without notifying Plaintiff and without obtaining her express written consent.

22. Plaintiff has a continuing interest in ensuring that Plaintiff's User Data, which, upon information and belief, remain backed up in RadNet's possession, is protected, and safeguarded from future breaches.

V. FACTUAL ALLEGATIONS

A. Radnet's Website and Privacy Policy

23. Defendant operates a website in the U.S. accessible from a desktop and mobile device at *radnet.com*.

24. Defendant provides its patients with a website, *radnet.com*, that includes an online patient portal through which patients can manager their health care needs. For example, through the online patient portal, patients can communicate with their healthcare providers, schedule appointments, pay bills, and view

information about past and upcoming appointments. Patients can also view their clinical notes, electronic health information, medical records, and test results, as soon as they become available, and access other healthcare related services.

25. Defendant encourages its patients to use its online patient portal.

26. Patients access the patient portal through the *radnet.com* website by logging in with their username and password.

27. RadNet's Website Privacy Policy in effect prior to the 2023 update, attached as **Exhibit 1**, represented that Defendant "respects the privacy of everyone who uses our Web site." Indeed, it touted RadNet's "commitment to ensuring that privacy."

28. The Website Privacy Policy promises that "You may rest assured that any further confidential information obtained, such as medical records and test results, will not be shared with anyone other than the appropriate and authorized RadNet staff, medical physicians, and payors."

29. The Website Privacy Policy also indicates that "any information [RadNet] obtained, which is limited to names and e-mail addresses, will be used solely for internal objectives, such as creating user profiles and for other RadNet marketing purposes."

30. Further, RadNet's Website Privacy Policy purports to include an opt-out provision for "information used for purposes not directly related to the RadNet

Web site" and represents that "Users are also notified when their information is being collected by any outside parties."

31. Notwithstanding these promises, RadNet deployed Facebook's Pixel on its website and patient portal that caused the contemporaneous unauthorized transmission of User Data and the precise content of patient communications with RadNet's patient portal to Facebook whenever a patient uses the patient portal.

B. How RadNet Intercepts and Discloses Patients' Personally Identifiable Information and Protected Health Information

i. Tracking Pixels

32. Websites and apps use Facebook's Pixel and SDK to collect information about user's devices and activities and send that to Facebook. Facebook then uses that information to show the user targeted ads.

33. The Facebook tracking Pixel, also known as a "tag" or "web beacon" among other names, is an *invisible* tool that tracks consumers' actions on Facebook advertisers' websites and reports them to Facebook. It is a version of the social plugin that gets "rendered" with code from Facebook. To obtain the code for the pixel, the website advertiser tells Facebook which website events it wants to track (e.g., messaging a healthcare provider or scheduling appointments) and Facebook returns corresponding Facebook Pixel code for the advertiser to incorporate into its website.

34. Through this technology, Facebook intercepts each page a user visits, what buttons they click, as well as specific information they input into the website

and what they searched. The Facebook Pixel sends each of these pieces of information to Facebook with PII, such as the user's IP address. Facebook stores this data on its own server, and, in some instances, for years on end.[1]

35. The Pixel harvests this data – even when a user is not logged into Facebook.[2]

36. Unbeknownst to Plaintiff and Class Members, Defendant installed the Facebook Pixel, not only on its website, but also on the portal that patients use to communicate sensitive, non-public, personal and health information to Defendant. As implemented by Defendant, the tracking Pixel was configured to collect and transmit the User Data of Plaintiff and Class Members to Facebook without their knowledge or consent.

37. Defendant installed the Facebook tracking Pixel, which enables it to intercept and disclose Plaintiff's and Class Members' User Data to Facebook, because it benefits financially from the advertising analytics and information services that stem from use of the Pixel. For example, in exchange for installing the pixel, Facebook provides Defendant with analytics about the ads they've placed on Facebook and Instagram and insight on other tools to target people who've visited their website.

[1] Grace Oldham and Dhruv Mehrotra, *Facebook and Anti-Abortion Clinics Are Collecting Highly Sensitive Info on Would-Be Patients*, The Markup (June 15, 2022), https://themarkup.org/pixel-hunt/2022/06/15/facebook-and-anti-abortion-clinics-are-collecting-highly-sensitive-info-on-would-be-patients (last visited Feb. 14, 2023).

[2] *Id*.

38. When a RadNet patient uses its patient portal to schedule an appointment, access test results, review diagnoses, or conducts any action, the website sends certain information about the patient to Facebook, including, but not limited to, their identity and specific communications and health procedures they underwent. Accordingly, the Pixel allows RadNet to intercept and disclose sensitive User Data.

ii. Facebook ID ("FID")

39. An FID is a unique and persistent identifier that Facebook assigns to each user. With it, anyone ordinary person can look up the user's Facebook profile and name. When a Facebook user with one or more personally identifiable FID cookies on his or her browser uses RadNet's patient portal, through its website code, causes the patient's User Data to be transmitted to Facebook by the user's browser. This transmission is not the patient's decision, but results from Defendant's purposeful use of the Facebook tracking pixel by incorporation of that pixel and code into the RadNet patient portal.

40. Defendant could easily program its website to prevent its patients' User Data from being automatically transmitted to Facebook when a patient logs in and uses the portal. However, it is not in Defendant's financial interest to do so because it benefits financially by providing this highly sought-after information.

41. Notably, while Facebook can easily identify any individual on its Facebook platform with only their unique FID, so too can any ordinary person who

comes into possession of an FID. Facebook admits as much on its website. Indeed, ordinary persons who come into possession of the FID can connect to any Facebook profile. Simply put, with only an FID and the sensitive User Data—all of which Defendant knowingly and readily provides to Facebook without any consent from patients—any ordinary person can connect the identity of the Facebook user profile with the types of medical procedures the patient underwent, and even access the patient's doctor's notes from Defendant.

42. At all relevant times, Defendant knew that the Facebook Pixel intercepted and disclosed User Data to Facebook. This was evidenced from, among other things, the functionality of the Pixel, i.e., sending all interactions and communications on its website to Facebook.

C. RadNet Health Unlawfully Discloses Its Patients' Personally Identifiable Patient Information and Protected Health Information to Facebook

43. RadNet maintains a vast digital database comprised of its patients' User Data, including the names and e-mail addresses of each patient, and their confidential medical records.

44. RadNet is not sharing anonymized, non-personally identifiable data with Facebook. To the contrary, the data it discloses is tied to unique identifiers that track specific Facebook users. Importantly, the recipient of the User Data—Facebook—*receives the information as one data point*. Defendant has thus monetized its database by disclosing its patients' PHI to Facebook in a manner allowing it to make a direct connection to patients' personal identities—without the

consent of its patients and to the detriment of their legally protected privacy and medical rights.

45. Critically, the User Data Defendant discloses to Facebook allows Facebook to build from scratch or cross-reference and add to the data it already has in their own detailed profiles for its own users, adding to its trove of personally identifiable data.

46. In June 2022, an investigation by The Markup revealed that the Facebook Pixel is embedded on the websites of 33 of the top 100 hospitals in the nation, collecting User Data, and transmitting it to Facebook when a user interacts with the website. For example, when a patient schedules an appointment online, the pixel intercepted and transmitted the details of the patient's doctor appointment, including the doctor's name, and search term used to find the doctor.[3]

47. Worse, this surveillance persisted even inside the password-protected patient portals, like RadNet's portal, of at least seven health systems. When a user navigates through their patient portal, the tracking Pixel collects intimate patient details, such as prescriptions, sexual orientation, and health conditions, and sends that data to Facebook.[4]

48. The 33 hospitals found to have the Facebook Pixel collecting and sending patient appointment details to Facebook collectively reported more than 26

[3] *Id.*
[4] *Id.*

million patient admissions and outpatient visits in 2020 alone. But the number of impacted patients is likely higher as The Markup's investigation was limited to just over 100 hospitals.

49. As a result of Defendant's data compiling and sharing practices, Defendant has knowingly disclosed to Facebook (for its own personal profit) the User Data of its patients.

50. Defendant does not seek its patients' prior written consent to the disclosure of their User Data (in writing or otherwise) and its patients remain unaware that their User Data is being disclosed to Facebook.

51. Plaintiff and Class Members had no way of knowing that Defendant was disclosing, and Facebook was intercepting, their User Data, including sensitive medical information, when they engaged with RadNet's website because the software is inconspicuously incorporated in the background.

52. This undisclosed conduct is even more egregious given the nature of the information entered in the RadNet patient portal, e.g., PII, test and lab results, requests for appointments, messages to health care providers, and other health information, among other things. Plaintiff and Class Members would not expect this information would be disclosed or intercepted without their consent. This is especially true given RadNet's consistent representations that this information would remain private and confidential.

53. Plaintiff and Class Members could not consent to RadNet's conduct when they were never aware their sensitive medical information would be disclosed to and intercepted by Facebook.

D. Defendant Does Not Need to Disclose Personally Identifiable Patient Information and Protected Health Information to Operate its Website and App

54. Tracking pixels are not necessary for Defendant to operate its website and patient portal. They are deployed on Defendant's website for the sole purpose of enriching Defendant and Facebook.

55. Even if a healthcare provider found it useful to integrate Facebook tracking pixels, Defendant is not required to disclose User Data to Facebook. In any event, if Defendant wanted to do so, it must first comply with the federal and state privacy laws described herein, which it failed to do.

E. Defendant Had an Obligation to Protect its Patients' Personally Identifiable Patient Information and Protected Health Information

56. Defendant has a legal duty to maintain its patient's User Data as confidential and to protect Plaintiff's and Class Members' User Data from disclosure to third parties.

57. Defendant's failure to adequately secure Plaintiff's and Class Members' sensitive User Data breaches duties it owes Representative Plaintiff and Class Members under statutory and common law.

58. Under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), health insurance providers have an affirmative duty to keep patients'

User Data private. As a covered entity, Defendant has a statutory duty under HIPAA and other federal and state statutes to safeguard Plaintiff's and Class Members' User Data. Moreover, Plaintiff and Class Members surrendered their highly sensitive personal data to Defendant under the implied condition that Defendant would keep it private and secure. Accordingly, Defendant also has an implied duty to safeguard their data, independent of any statute.

59. Because Defendant is covered by HIPAA (45 C.F.R. § 160.102), it is required to comply with the HIPAA Privacy Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C.

60. HIPAA's Privacy Rule or Security Standards for Privacy of Individually Identifiable Health Information establishes national standards for the protection of health information, including health information that is kept or transferred in electronic form.

61. HIPAA requires Defendant to "comply with the applicable standards, implementation specifications, and requirements" of HIPAA "with respect to electronic protected health information." 45 C.F.R. § 164.302.

62. "Electronic protected health information" is "individually identifiable health information … that is (i) transmitted by electronic media; maintained in electronic media." 45 C.F.R. § 160.103.

63. HIPAA's Security Rule requires Defendant to do the following:

a) Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits;

b) Protect against any reasonably anticipated threats or hazards to the security or integrity of such information;

c) Protect against any reasonably anticipated uses or disclosures of such information that are not permitted; and

d) Ensure compliance by its workforce.

64. HIPAA also requires Defendant to "review and modify the security measures implemented … as needed to continue provision of reasonable and appropriate protection of electronic protected health information" under 45 C.F.R. § 164.306(e), and to "[i]mplement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights." 45 C.F.R. § 164.312(a)(1).

65. In addition to its obligations under federal and state laws, Defendant owed a duty to Plaintiff and Class Members to exercise reasonable care in obtaining,

retaining, securing, safeguarding, deleting, and protecting the User Data in Defendant's possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Defendant owed a duty to Plaintiff and Class Members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that its computer systems, networks, and protocols adequately protected the User Data of Plaintiff and Class Members.

F. Plaintiff and Class Members Have a Reasonable Expectation of Privacy in Their User Data

66. Plaintiff and Class Members have a reasonable expectation of privacy in their User Data, including sensitive medical information.

67. Privacy polls and studies uniformly show that most Americans consider one of the most important privacy rights to be the need for an individual's affirmative consent before a company collects and shares its customers' personal data.

68. For example, a recent study by Consumer Reports shows that 92% of Americans believe that internet companies and websites should be required to obtain consent before selling or sharing consumers' data, and the same percentage believe internet companies and websites should be required to provide consumers with a complete list of the data that has been collected about them.

69. Moreover, according to a study by Pew Research Center, a majority of Americans, approximately 79%, are concerned about how data is collected about them by companies.

70. Users act consistent with these preferences. Following a new rollout of the iPhone operating software—which asks users for clear, affirmative consent before allowing companies to track users—85% of worldwide users and 94% of U.S. users chose not to share data when prompted.

71. Another recent study by DataGrail revealed that 67% of people were willing to pay $100 or more annually to keep their information out of the hands of companies and the government.

72. The same study revealed that 75% of people would abandon brands that do not take care of their data.

73. Other privacy law experts have expressed concerns about the disclosure to third parties of a user's sensitive medical information. For example, Dena Mendelsohn—the former Senior Policy Counsel at Consumer Reports and current Director of Health Policy and Data Governance at Elektra Labs—explained that having your personal health information disseminated in ways you are unaware of could have serious repercussions, including affecting your ability to obtain life insurance and how much you pay for that coverage, increasing the rate you are charged on loans, and leaving you vulnerable to workplace discrimination.

G. The Data RadNet Intercepted is Plaintiff's Property, Has Economic Value, and its Unlawful Disclosure Caused Economic Harm

74. There is an economic market for consumers' personal data—including the User Data RadNet allowed Facebook to intercept from Plaintiff and Class Members.

75. For instance, according to Experian, health data is a "gold mine" for health care companies and clinicians.

76. In 2013, the Financial Times reported that the data-broker industry profits from the trade of thousands of details about individuals, and within that context, "age, gender and location" information are sold for about "$0.50 per 1,000 people."[5] This estimate was based upon "industry pricing data viewed by the Financial Times," at the time.[6]

77. In 2015, TechCrunch reported that "to obtain a list containing the names of individuals suffering from a particular disease," a market participant would have to spend about "$0.30 per name."[7] That same article noted that "Data has become a strategic asset that allows companies to acquire or maintain a competitive edge"[8] and that the value of a single user's data (within the corporate acquisition context) can vary from $15 to more than $40 per user.[9]

78. Notably, a 2021 report from Invisibly found that personal medical information is one of the most valuable pieces of data within this data-market. "It's worth acknowledging that because health care records often feature a more complete collection of the patient's identity, background, and PII, health care records have

[5] Emily Steel, et al., *How much is your personal data worth?*, Fin. Times (June 12, 2013), https://ig.ft.com/how-much-is-your-personal-data-worth/#axzz3myQiwm6u.
[6] *Id.*
[7] Pauline Glickman and Nicolas Glady, *What's the Value of Your Data?*, TechCrunch (October 13, 2015), https://techcrunch.com/2015/10/13/whats-the-value-of-your-data/.
[8] *Id.*
[9] *Id.*

proven to be of particular value for data thieves. While a single social security number might go for $0.53, a complete health care record sells for $250 on average. For criminals, the more complete a dataset, the more potential value they can get out of it. As a result, healthcare breaches increased 55% in 2020."[10] The article noted the following breakdown in average price for record type:

Record Type	Average Price
Health Care Record	$250.15
Payment Card Details	$5.40
Banking Records	$4.12
Access Credentials	$0.95
Social Security Number	$0.53
Credit Record	$0.31
Basic PII	$0.03

79. The Federal Trade Commission has also confirmed the value of user data and, particularly, health information. In 2014, it found that data brokers sell data that categorize users into sensitive categories, such as "expectant parent."[11] It recently sued one of these companies for selling location data on people who visit abortion clinics for approximately $160 a week.

[10] *How Much is Your Data Worth? The Complete Breakdown for 2021*, Invisibly (July 13, 2021), https://www.invisibly.com/learn-blog/how-much-is-data-worth/.

[11] FTC, *Data Brokers: A Call for Transparency and Accountability* (May 2014), https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability- report-federal-trade-commission-may-2014/140527databrokerreport.pdf.

80. Indeed, even access to just prescription information is extremely valuable. For instance, Datarade.ai advertises access to U.S. customers names, addresses, email addresses, telephone numbers who bought brand name medicine. The starting price for access to just some of this data was $10,000. Other companies, like Pfizer, spend $12 million annually to purchase health data and the medical data industry itself was valued at over $2.6 billion back in 2014.

81. Furthermore, individuals can sell or monetize their own data if they so choose. A myriad of other companies and apps such as Nielsen Data, Killi, DataCoup, and AppOptix offer consumers money in exchange for their personal data.

82. Moreover, "courts have recognized the 'growing trend across courts . . . to recognize the lost property value' of personal information. *In re Marriott Int'l, Inc., Cust. Data Sec. Breach Litig.*, 440 F.Supp.3d 447, 461 (D. Md. 2020) . . .; *see also In re Facebook Privacy Litigation*, 557 F.App'x. 494, 494 [sic] (9th Cir. 2014)." *Calhoun v. Google LLC*, 526 F.Supp.3d 605, 636 (N.D. Cal. 2021)."

83. Given the monetary value already assigned to personal information, RadNet has deprived Plaintiff and Class Members of the economic value of their sensitive medical information by acquiring such data without providing proper consideration for Plaintiff's and Class Members' property.

VI. TOLLING, CONCEALMENT, AND ESTOPPEL

84. The applicable statutes of limitation have been tolled as a result of RadNet's knowing and active concealment and denial of the facts alleged herein.

85. RadNet secretly incorporated the Facebook Pixel into its website and patient portal, providing no indication to users that their User Data, including PII and medical information, would be disclosed to Meta.

86. RadNet possessed exclusive knowledge that the Facebook Pixel was incorporated on its website and patient portal, yet failed to disclose that fact to users, or that by interacting with its website and patient portal Plaintiff's and Class Members' User Data, including PII and health data, would be disclosed to Facebook.

87. Plaintiff and Class Members could not with due diligence have discovered the full scope of RadNet's conduct, including because the incorporation of the Facebook Pixel is surreptitious, highly technical and there were no disclosures or other indication that would inform a reasonable consumer that RadNet was disclosing to and allowing the interception of User Data, including PII and health data, by Facebook.

88. The earliest Plaintiff and Class Members could have known about Defendant's conduct was shortly before the filing of this Complaint.

89. RadNet was under a duty to disclose the nature and significance of its data disclosure practices but did not do so. RadNet is therefore estopped from relying on any statute of limitations under the discovery rule.

90. Additionally, RadNet engaged in fraudulent conduct to prevent Plaintiff and Class Members from discovering the disclosure and interception of their data. RadNet misled Plaintiff and Class Members to believe their User Data, including health information and PII, would not be disclosed.

91. Plaintiff and Class Members were not aware that RadNet disclosed their User Data, including PII and health information.

92. Plaintiff and Class Members exercised due diligence to uncover the facts alleged herein and did not have actual or constructive knowledge of RadNet's misconduct by virtue of their fraudulent concealment.

93. Accordingly, all statutes of limitations are tolled under the doctrine of fraudulent concealment.

VII. CLASS ACTION ALLEGATIONS

94. Plaintiff brings this action on behalf of herself and all others similarly situated as a class action under Rules 23(a) and (b)(3) of the Federal Rules of Civil Procedure, on behalf of the following Classes (collectively, the "Class"):

> **Nationwide Class:** All persons in the United States who are, or were patients of Defendant, and accessed an online website owned and/or operated by Defendant that caused a transmission of personally identifiably information, PHI, and other electronic communications to be made to Facebook.
>
> **California Subclass:** All California persons who are, or were patients of Defendant, and accessed an online website owned and/or operated by Defendant that caused a transmission of personally identifiably information, PHI,

and other electronic communications to be made to Facebook.

Excluded from the Classes are Defendant, their past or current officers, directors, affiliates, legal representatives, predecessors, successors, assigns and any entity in which any of them have a controlling interest, as well as all judicial officers assigned to this case as defined in 28 USC § 455(b) and their immediate families.

95. Numerosity. Members of the Classes are so numerous that joinder of all members of the Class is impracticable. The exact number of Class Members is unknown to Plaintiff at this time; however, it is estimated that there are thousands of individuals in the Classes. Class Members can be readily identified from Defendant's records and non-party Facebook's records.

96. Typicality. Plaintiff's claims are typical of the claims of Members of the Classes. Plaintiff and Members of the Classes were harmed by the same wrongful conduct by Defendant in that they used Defendant's website and had their User Data intercepted and disclosed to Facebook without Plaintiff's or Class Members' knowledge, express written consent, or authorization. Plaintiff's claims are based on the same legal theories as the claims of other Class Members.

97. Adequacy. Plaintiff will fairly and adequately protect and represent the interests of the members of the Class. Plaintiff's interests are coincident with, and not antagonistic to, those of the members of the Class. Plaintiff is represented by counsel with experience in the prosecution of class action litigation generally and in the emerging field of digital privacy litigation specifically.

98. Commonality. Questions of law and fact common to the Members of the Classes predominate over questions that may affect only individual Members of the Classes because Defendant has acted on grounds generally applicable to the Classes. Such generally applicable conduct is inherent in Defendant's wrongful conduct. Questions of law and fact common to the Classes include:

a) Whether Defendant had a duty to protect and refrain from disclosing Plaintiff's and Class Members' User Data;

b) Whether Defendant knowingly intercepted and/or disclosed Plaintiff and Class Members' User Data to Facebook;

c) Whether Defendant negligently maintained its records containing Plaintiff and Class Members' User Data;

d) Whether Plaintiff and Class Members authorized or consented to Defendant's disclosure of their User Data to Facebook;

e) Whether Defendant's acts and practices violated the CIPA;

f) Whether Defendant's acts and practices violated the CIMA;

g) Whether Defendant's actions violate Plaintiff's and Class Members' privacy rights as provided by the California Constitution and the common law;

h) Whether Defendant breached its contract with Plaintiff and Class Members;

i) Whether Plaintiff and Class Members are entitled to equitable relief, including but not limited to, injunctive relief, restitution, and disgorgement; and

j) Whether Plaintiff and the Class Members are entitled to actual, statutory, punitive or other forms of damages, and other monetary relief.

99. Superiority. Class action treatment is a superior method for the fair and efficient adjudication of the controversy. Such treatment will permit a large number of similarly situated persons to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, or expense that numerous individual actions would engender. The benefits of proceeding through the class mechanism, including providing injured persons or entities a method for obtaining redress on claims that could not practicably be pursued individually, substantially outweighs potential difficulties in management of this class action. Plaintiff knows of no special difficulty to be encountered in litigating this action that would preclude its maintenance as a class action.

100. Plaintiff reserves the right to revise the foregoing class allegations and definitions based on facts learned and legal developments following additional investigation, discovery, or otherwise.

VIII. CLAIMS FOR RELIEF

FIRST CLAIM FOR RELIEF
Violation of the California Invasion of Privacy Act ("CIPA")
Cal. Penal Code § 630, *et seq*.
(On Behalf of Plaintiff and the California Subclass)

101. Plaintiff incorporates paragraphs 1 through 100 by reference as if fully set forth herein.

102. The CIPA was enacted to safeguard privacy from new technologies in the ever-evolving digital age. The Act begins with its statement of purpose:

> The Legislature hereby declares that advances in science and technology have led to the development of new devices and techniques for the purpose of eavesdropping upon private communications and that the invasion of privacy resulting from the continual and increasing use of such devices and techniques has created a serious threat to the free exercise of personal liberties and cannot be tolerated in a free and civilized society."

Cal. Penal Code § 630.

103. To establish liability under Section 631(a), a plaintiff need only establish that the Defendant, "by means of any machine, instrument, or contrivance, or any other manner," does any of the following:

> *intentionally taps, or makes any unauthorized connection*, whether physically, *electrically*, acoustically, inductively, or otherwise, with any telegraph or telephone wire, line, cable*, or instrument*, including the wire, line, cable, or instrument of any internal telephonic communication system; or
>
> *willfully and without the consent of* ***all*** *parties to the communication, or in any unauthorized manner*, *reads, or attempts to read, or to learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line, or cable, or is being sent from, or received at any place within this state*; *or*
>
> *uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained, or who aids, agrees with, employs, or conspires with any person or persons to unlawfully do, or permit, or cause to be done any of the acts or things mentioned above in this section.*

Cal. Penal Code § 631(a) (emphasis added).

104. Section 631(a) is not limited to phone lines, but also applies to "new technologies" such as computers, the Internet, and email. *See Matera v. Google Inc.*, No. 15-cv-4062-LHK, 2016 WL 8200619, at *21 (N.D. Cal. Aug. 12, 2016) (CIPA applies to "new technologies" and must be construed broadly to effectuate its remedial purpose of protecting privacy); *Bradley v. Google, Inc.*, No. 06-cv- 5289-WHA, 2006 WL 3798134, at *5-6 (N.D. Cal. Dec. 22, 2006) (CIPA governs "electronic communications"); *In re Facebook, Inc. Internet Tracking Litigation*, 956 F.3d 589 (9th Cir. 2020) (reversing dismissal of CIPA and common law privacy claims based on Facebook's collection of consumers' internet browsing history).

105. To avoid liability under the CIPA, a Defendant must show it had the consent of ***all*** parties to a confidential communication. Cal. Penal Code § 632.

106. As described in the statute, a "confidential communication" is "any communication carried on in circumstances as may reasonably indicate that any party to the communication desired it to be confided to the parties thereto[.]" *Id*.

107. Defendant aided, agreed with, employed, and conspired with Facebook to track and intercept Plaintiff's and Class Members' internet communications while accessing Defendant's website—without their authorization and consent.

108. Defendant, in aiding and assisting Facebook's eavesdropping of Plaintiff and Class Members, intended to help Facebook learn or attempt to learn the meaning of the contents of or record the confidential communications at issue.

109. The patient communication information that Defendant transmitted to Facebook, through its Pixel, such as messages with healthcare providers, appointment scheduling, constitutes protected health information.

110. As demonstrated herein, Defendant violated CIPA by aiding and permitting third parties to receive its patients' online communication through its website without their consent.

111. By disclosing Plaintiff's and the Class Members' User Data Defendant violated Plaintiff's and Class Members' statutorily protected right to privacy.

112. As a result of the above violations, Defendant is liable to the Plaintiff and Class Members for actual damages related to their loss of privacy in an amount to be determined at trial or alternatively for "liquidated damages not less than $2,500 per plaintiff." Pursuant to CIPA Section 637.2, any person who has been injured by a violation of CIPA may recover $5,000 dollars per violation or three times the amount of actual damages (the greater of these two options). Additionally, Section 637.2 specifically states that "[it] is not a necessary prerequisite to an action pursuant to this section that the plaintiffs has suffered, or be threatened with, actual damages."

113. Under the CIPA, Defendant is also liable for reasonable attorney's fees, and other litigation costs, injunctive and declaratory relief, and punitive damages in an amount to be determined by a jury, but sufficient to prevent the same or similar conduct by the Defendant in the future.

SECOND CLAIM FOR RELIEF

Violation of the California Confidentiality of Medical Information Act ("CMIA")
Cal. Civ. Code §§ 56.10 & 56.35 – Disclosure of Medical Information
(On Behalf of Plaintiff and the California Subclass)

114. Plaintiff incorporates the paragraphs 1 through 100 by reference as if fully set forth herein.

115. Under the CMIA section 56.10, providers of health care are prohibited from disclosing medical information relating to their patients, without a patient's authorization. Medical information refers to "any individually identifiable information, in electronic or physical form, in possession of or derived from a provider of health care . . . regarding a patient's medical history, mental or physical condition, or treatment. 'Individually Identifiable' means that the medical information includes or contains any element of personal identifying information sufficient to allow identification of the individual . . . ." Cal. Civ. Code § 56.05.

116. Defendant is deemed a provider of health care under Cal. Civ. Code. Section 56.06, subdivision (a) and (b), because it "maintain[s] medical information" of patients and makes it available for the "purposes of allowing its users to manage his or her information" or for the diagnosis, treatment, or management of a medical condition. Cal. Civ. Code. § 56.06.

117. Defendant is therefore subject to the requirements of the CMIA and obligated under subdivision (b) to maintain the same standards of confidentiality required of a provider of health care with respect to medical information that it maintains on behalf of patients.

118. Plaintiff and Class Members are patients, and, as a health care provider, Defendant has an ongoing obligation to comply with the CMIA's requirements.

119. As described herein, Facebook ID is an identifier sufficient to allow identification of a specific individual. Along with patients' Facebook ID, Defendant discloses to Facebook—without first obtaining authorization—several pieces of information regarding its patients' use of its website, which includes, but is not limited to: patient medical records, medical conditions, medical concerns, treatment patients are seeking, email address, address, telephone number, etc. As a result, Defendant violated Civil Code section 56.10, subdivision (a).

120. This patient information is derived from a provider of healthcare regarding patients' medical treatment and physical condition. Accordingly, it constitutes medical information pursuant to the CMIA.

121. As demonstrated herein, Defendant failed to obtain its patients' authorization for the disclosure of medical information and failed to disclose in its Privacy Policy that it shares protected health information for marketing purposes.

122. Pursuant to CMIA section 56.11, a valid authorization for disclosure of medical information must, *inter alia*, be (1) "clearly separate from any other language present on the same page and is executed by a signature which serves no other purpose than to execute the authorization" (2) signed and dated by the patient or their representative (3) state the name and function of the third party that receives the information (4) state a specific date after which the authorization expires.

Accordingly, the information set forth in Defendant's Privacy Policy does not qualify as valid authorization.

123. Defendant knowingly and willfully disclosed medical information without consent to Facebook for financial gain. Specifically, to market and advertise its services, or to allow others to market and advertise their services, in violation of Civil Code section 56.06 subdivisions (b) and (c).

124. California Civil Code § 56.35 provides that a patient who has sustained economic loss or personal injury resulting from the disclosure of his or her individually identifiable medical information, in violation of California Code § 56.10, may recover compensatory damages, punitive damages not to exceed $3,000, attorneys' fees, and costs of litigation. Accordingly, Plaintiff and Class Members are entitled to: (1) actual damages, in an amount to be determined at trial; (2) punitive damages; and (3) attorneys' fees and other litigation costs reasonably incurred.

THIRD CLAIM FOR RELIEF
Violation of the California Confidentiality of Medical Information Act ("CMIA")
Cal. Civ. Code §§ 56.101 & 56.36 – Negligent Preservation of Medical Records
(On Behalf of Plaintiff and the California Subclass)

125. Plaintiff incorporates the paragraphs 1 through 100 by reference as if fully set forth herein.

126. The CMIA requires that every provider of health care who "creates, maintains, preserves, stores, abandons, destroys, or disposes of medical information

shall do so in a manner that preserves the confidentiality of the information contained therein." Cal. Civ. Code § 56.101.

127. Any healthcare provider who "negligently creates, maintains, preserves, stores, abandons, destroys, or disposes of medical information shall be subject to the remedies and penalties provided under subdivisions (b) and (c) of Section 56.36."

128. Defendant failed to maintain, preserve, and store medical information in a manner that preserves the confidentiality of the information contained therein because it disclosed Plaintiff's and Class Members' sensitive medical information without consent, including information concerning their medical condition, diagnoses, treatment, appointment information, as well as personally identifiable patient information, such as patients' FID.

129. Defendant's failure to maintain, preserve, and store medical information in a manner that preserves the confidentiality of the information was, at the least, negligent and violates California Civil Code section 56.06 subdivisions (b) and (c).

130. Accordingly, Plaintiff and Class Members are entitled to the penalties and remedies provided under subdivisions (b) and (c) of Section 56.35, including (1) nominal damages of $1,000 per violation; (2) actual damages, in an amount to be determined at trial; and (3) reasonable attorneys' fees and other litigation costs reasonably incurred.

FOURTH CLAIM FOR RELIEF
Invasion of Privacy Under the California Constitution and Common Law
(On Behalf of Plaintiff and the California Subclass)

131. Plaintiff incorporates paragraphs 1 through 100 by reference as if fully set forth herein.

132. Plaintiff and Class Members have a legally protected privacy interest in the User Data that they enter into Defendant's Website and are entitled to the protection of their information and property against unauthorized access.

133. For reasons detailed above, Plaintiff and Class Members reasonably expected that their User Data would be protected and secure from unauthorized parties, and that it would not be disclosed to any unauthorized parties or disclosed for any improper purpose.

134. Defendant unlawfully invaded the privacy rights of Plaintiff and Class Members by: (a) disclosing their private, and personal information to unauthorized parties in a manner that is highly offensive to a reasonable person; and (b) disclosing their private and personal information to unauthorized parties without the informed and clear consent of Plaintiff and Class Members, including but not limited to including the Facebook Pixel and other tracking code on its website that transfer information entered and records of actions taken by patients on Defendant's website to unrelated entities. This invasion into the privacy interest and seclusion of Plaintiff and Class Members is serious and substantial.

135. In willfully sharing Plaintiff's and Class Members' Personal Information, Defendant acted in reckless disregard of their privacy rights.

136. Defendant violated Plaintiff's and Class Members' right to privacy under California law, including, but not limited to California common law and Article 1, Section 1 of the California Constitution and the California Consumer Privacy Act.

137. As a direct and proximate result of Defendant's unlawful invasions of privacy, Plaintiff's and Class Members' private, personal, and confidential information has been accessed or is at imminent risk of being accessed, and their reasonable expectations of privacy have been intruded upon and frustrated. Plaintiff and proposed Class Members have suffered injuries as a result of Defendant's unlawful invasions of privacy and are entitled to appropriate relief.

138. Plaintiff and Class Members are entitled to injunctive relief as well as actual damages, punitive damages, and damages for invasion of their privacy rights in an amount to be determined by a jury without reference to specific economic harm.

FIFTH CLAIM FOR RELIEF
Breach of Contract
(On Behalf of Plaintiff and the Classes)

139. Plaintiff incorporates the paragraphs 1 through 100 by reference as if fully set forth herein.

140. As shown above, Defendant expressly promised to safeguard Plaintiff's and Class Members' User Data, including their sensitive medical information, and to not disclose that data to third parties without their consent.

141. In addition to the express contract provisions set forth above, implied contracts existed between Defendant and Plaintiff that Defendant would not conspire with others to violate Plaintiff's legal rights to privacy in their User Data.

142. Plaintiff and Class Members accepted Defendant's promises not to disclose their User Data without explicit consent and/or authorization when they entered into a contract with Defendant.

143. Plaintiff and Class Members fully performed their obligations under their contract with Defendant, including by providing their User Data and paying for medical services and/or treatment.

144. Defendant did not hold up its end of the bargain. Defendant secretly disclosed Plaintiff and Class Members' User Data, including sensitive medical information, to Facebook, without consent in violation of their agreement with Plaintiff and Class Members.

145. Plaintiff and Class Members would not have entrusted Defendant with their User Data in the absence of a contract between them and Defendant's express promise not to disclose this information.

146. As a direct and proximate result of Defendant's breach of their contract, Plaintiff and Class Members sustained damages as alleged herein. Plaintiff and Class

Members would not have used Defendant's services, or would have paid substantially less for these services, had they known their User Data would be disclosed.

147. Plaintiff and Class Members are entitled to the following damages: (a) nominal damages for breach of contract; (b) general damages for invasion of their privacy rights without reference to specific economic harm; (c) compensatory or consequential damages caused by (i) the fact that sensitive and confidential health and personal information that Plaintiffs and Class Members intended to keep private are no longer private; (ii) Defendant's erosion of the essential confidential nature of the patient-provider relationship; and (iii) the thing of value taken from Plaintiff and Class Members, and benefits derived therefrom, without Plaintiff and Class Members' knowledge or informed consent and without sharing the benefit of such value.

SIXTH CLAIM FOR RELIEF
Unjust Enrichment
(In the Alternative)
(On Behalf of Plaintiff and the Classes)

148. Plaintiff incorporates the paragraphs 1 through 100 by reference as if fully set forth herein.

149. Plaintiff and Class members conferred a benefit upon Defendant in the form of valuable sensitive medical information that Defendant collected from Plaintiff and Class members under the guise of keeping this information private. Defendant collected and used this information for its own gain, including

advertisement purposes or sale. Additionally, Plaintiff and Class members conferred a benefit upon Defendant in the form of monetary compensation.

150. Plaintiff and Class members would not have used Defendant's services, or would have paid less for these services, if they had known Defendant would use and disclose this information.

151. Defendant unjustly retained those benefits at the expense of Plaintiff and Class members because Defendant's conduct damaged Plaintiff and Class members, all without providing any commensurate compensation to Plaintiff and Class members.

152. The benefits that Defendant derived from Plaintiff and Class members rightly belong to Plaintiff and Class members. It would be inequitable under unjust enrichment principles in California and every other state for Defendant to be permitted to retain any of the profit or other benefits they derived from the unfair and unconscionable methods, acts, and trade practices alleged in this Complaint.

153. Defendant should be compelled to disgorge in a common fund for the benefit of Plaintiff d Class members all unlawful or inequitable proceeds that Defendant received, and such other relief as the Court may deem just and proper.

IX. RELIEF REQUESTED

154. Accordingly, Plaintiff, on behalf of herself and the proposed Classes, respectfully requests that this Court:

a) Determine that this action may be maintained as a class action pursuant to Rules 23(a), and (b)(3) of the Federal Rules of Civil Procedure, direct that reasonable notice of this action, as provided by Rule 23(c)(2), be given to the Classes, and declare Plaintiff as the representative of the Classes and her counsel as Class Counsel;

b) Declare that Defendant's conduct, as set out above, violates the laws cited herein;

c) Award damages, including nominal, statutory, and punitive damages where applicable, to Plaintiff and the Classes in an amount to be determined at trial;

d) Award Plaintiff and the Classes their reasonably litigation expenses and attorneys' fees;

e) Awarding Plaintiff and the Classes pre-and post-judgment interest, to the extent allowable;

f) Awarding such other further injunctive and declaratory relief as is necessary to protect the interests of Plaintiff and the Classes; and

g) Awarding such other and further relief as the Court deems reasonable and just.

JURY DEMAND

Pursuant to Rule 38 of the Federal Rules of Civil Procedure, Plaintiff, on behalf of herself and the proposed Class, demands a trial by jury on all issues so triable.

Dated: March 23, 2023

Respectfully submitted,

EDELSBERG LAW, P.A.

/s/ Scott Edelsberg, Esq.
Scott Edelsberg, Esq.
CA Bar No. 330090
scott@edelsberglaw.com
1925 Century Park East, Suite 1700
Los Angeles, CA 90067
Tel: 305-975-3320

Counsel for Plaintiff and the Proposed Class